

1AP20 Rec'd PCT/PTO 21 APR 2006

## SCHUTZ VOR UNERWÜNSCHTEN NACHRICHTEN

Gebiet der Erfindung

- 5 Die vorliegende Erfindung betrifft allgemein das Gebiet der Kommunikationstechnologie und insbesondere eine Überwachung von Nachrichten, speziell im Zusammenhang mit an Kinder gesendeten unerwünschten E-Mails.

10 Hintergrund der Erfindung

- In modernen Kommunikationsumgebungen können Nachrichten einem Empfänger bereitgestellt werden, die dieser nicht erhalten soll. Insbesondere ist es bei computerbasierten  
15 Kommunikationsumgebungen, wie zum Beispiel dem Internet, bekannt, dass Nachrichten in Form von E-Mails Empfängern bereitgestellt werden, die diese nicht erhalten sollen.

- So besteht ein Problem beispielsweise darin, dass Kinder  
20 beim Benutzen eines E-Mail-Accounts im Internet unerwünschte und unbekannte E-Mails erhalten. Diese E-Mails sind aber selten für diese junge Zielgruppe geeignet und können z. B. pornographische Inhalte, unseriöse Angebote wie z. B. Finanzdienstleistungen, Glücksspielangebote,  
25 unerwünschte Produktangebote, Angebote zu verschreibungspflichtigen Arzneimitteln etc. enthalten.

- Ein weiteres Problem ist, dass Eltern keine Kontrolle über das Kommunikationsverhalten ihrer Kinder haben und so ihre  
30 Kinder auch nicht vor unerwünschten und unbekannten E-Mails schützen können.

- Des Weiteren ist es unerwünscht, dass der Benutzer eines dienstlichen E-Mail-Accounts beispielsweise private E-Mails  
35 erhält, die nicht in den dienstlichen Rahmen fallen.

Im Bereich computerbasierter Netzwerkumgebungen und insbesondere bei über das Internet übertragenen E-Mails ist es bekannt, sogenannte Filter (z. B. Spamfilter) zu

BESTÄTIGUNGSKOPIE

verwenden, um den Empfang unerwünschter Nachrichten zu verhindern. Hier können zwei Ansätze unterschieden werden.

Bei einem Ansatz ist es möglich, Nachrichten in Form von E-Mails vor ihrer Übertragung zu einem vorgesehenen Empfänger auf ihre Inhalte und Absender zu überprüfen und gegebenenfalls als unerwünscht erkannte E-Mails nicht dem Empfänger bereitzustellen. In diesem Fall erhält der Empfänger keine gemäß der verwendeten Filterung als unerwünscht erkannten E-Mails. Dies hat den Nachteil, dass der Empfänger keine Kenntnis darüber erhält, welche E-Mails als unerwünscht erkannt und dementsprechend nicht übertragen wurden. Daher ist es möglich, dass der Empfänger fälschlicherweise als unerwünscht klassifizierte E-Mails nicht erhält, also erwünschte E-Mails nicht bereitgestellt werden. Um dies zu verhindern, werden bei diesem Ansatz verwendete Filter üblicherweise so konfiguriert, dass E-Mails nur dann herausgefiltert und nicht bereitgestellt werden, wenn zweifelsfrei festgestellt werden kann, dass sie unerwünscht sind. Dies hat aber wiederum zur Folge, dass die Anzahl fälschlicherweise nicht als unerwünscht erkannter und dem Empfänger übertragener E-Mails hoch sein kann.

Aus der WO 99/37066 A1 sind ein Verfahren und Email-System zur Überwachung von an einen Empfänger adressierten Nachrichten bekannt, bei dem der Empfänger so eingerichtet wird, dass er eine Empfangseinrichtung aufweist, die unerwünschte Nachrichten (sog. „JUNK“) abfängt, damit diese den Empfänger nicht erreichen, d.h. dass dort bereits eine Empfangseinrichtung vom Typ „unerwünscht“ beschrieben ist. Im Einzelnen wird dort ein Empfangsfilter verwendet, der jede eingehende Nachricht mittels einer heuristischen Untersuchung überprüft, um festzustellen, ob die Nachricht unerwünscht sein könnte oder nicht. Diejenigen Nachrichten, die der Kategorie „unerwünscht“ zugeordnet werden, erhalten den sog. „JUNK“-Status und werden dem Benutzer nicht angezeigt, sondern automatisch vom System gelöscht. Demnach ist der hier beschriebene Empfänger so eingerichtet, dass Zugriffe eines Benutzers auf die Empfangseinrichtung

"unerwünscht" verhindert werden, indem sie nicht angezeigt werden. Und es ist dort bereits eine Nachrichtenkategorie „unerwünscht“ definiert, die solche Nachrichten angibt, für die verhindert werden soll, dass sie dem Benutzer  
5 bereitgestellt werden, wobei überprüft wird, ob eine Nachricht in diese Kategorie fällt und gegebenenfalls der Empfangseinrichtung „unerwünscht“ zugeordnet wird. Da der Benutzer keine Einsicht darin hat, welche Nachrichten vom System als „unerwünscht“ kategorisiert werden und für das  
10 automatische Löschen vorgesehen sind, besteht auch keine Möglichkeit hier evtl. manuell korrigierend einzugreifen. Vielmehr muss der Benutzer es hinnehmen, dass die vom System automatisch gelöschten Nachrichten unwiederbringlich verloren sind.

15 Aus der US 2002/0199095 A1 ist bekannt, ein „e-mail relay“ als einen zweiten Empfänger vorzusehen, der eingehenden Nachrichten vorfiltert, wobei drei verschiedene Nachrichtenkategorien definiert werden, nämlich „Clean“  
20 „Spam“ und „Borderline“ (s dort Fig. 2) und die Emails entsprechend unterschiedlich weiter behandelt werden. Die als „Clean“ kategorisierten Emails entsprechen erwünschten Nachrichten, die sogleich an den Empfänger zum Zugriff durch den Benutzer weitergeleitet werden. Die als „Spam“  
25 erkannten Emails sind unerwünschte Nachrichten, die nicht weitergeleitet werden, so dass der Benutzer darauf keinen Zugriff hat. Die schließlich als „Borderline“ bezeichneten Emails sind „ Grenzfälle“, d.h. Nachrichten die nicht sofort als „Clean“ oder „Spam“ erkannt werden und daher  
30 unbekannten Status haben. Diese unbekannten Nachrichten werden für eine weiteren Überprüfung („further review“) vorgesehen. Dazu werden diese Nachrichten von den anderen isoliert („quarantined“) und in einem Datenbankspeicher aufbewahrt, um später von einem Systemverwalter  
35 („administrator“) genauer untersucht werden zu können. Das bedeutet, dass der zweite Empfänger („e-mail relay“) so eingerichtet ist, dass er eine Empfangseinrichtung „unbekannt“ aufweist und den Zugriff darauf zumindest dem Benutzer („administrator“). Welche Zugriffsmöglichkeiten  
40 oder -beschränkungen für den ersten Empfänger und dessen

Benutzer bestehen, ist dort nicht näher beschrieben. Somit wird hier lediglich ein nicht ausreichender Lösungsansatz für das eingangs genannte Problem vorgeschlagen.

- 5 Außerdem kann ein weiterer Ansatz verwendet werden, der auch unabhängig von dem zuvor genannten Ansatz Verwendung findet. Hier erfolgt die Filterung von E-Mails so, dass alle an einen Empfänger adressierten E-Mails übertragen und dort in erwünschte und unerwünschte E-Mails klassifiziert  
10 werden. Als unerwünscht erkannte E-Mails werden nicht verworfen, sondern als unerwünscht gekennzeichnete E-Mails bereitgestellt. Dies kann beispielsweise dadurch erfolgen, dass erwünschte E-Mails einem ersten Ordner und unerwünschte E-Mails einem zweiten Ordner zugeordnet  
15 werden. Dies hat den Vorteil, dass der Empfänger gezielt auf erwünschte E-Mails zugreifen und dem zweiten Ordner zugeordnete, unerwünschte E-Mails außer Acht lassen kann. Im Gegensatz zu dem ersten Ansatz hat der Empfänger hier die Möglichkeit, durch Zugriff auf den zweiten Ordner zu  
20 überprüfen, ob diesem fälschlicherweise als unerwünscht erkannte E-Mails zugeordnet wurden. Dies hat aber wiederum einen Nachteil, da auf dem zweiten Ordner zugeordnete E-Mails zugegriffen werden kann. Daher ist es möglich, dass beispielsweise ein Minderjähriger Zugriff auf E-Mails  
25 erhält, die z. B. pornografische oder kriegsverherrlichende Inhalte haben.

Vergleichbare Probleme treten bei dienstlich genutzten E-Mail-Accounts auf. Auch hier ist es im Grundsatz lediglich  
30 möglich, unerwünschte E-Mails, beispielsweise E-Mails ohne dienstlichen Charakter, unter der Annahme einer korrekten Filterung nicht dem vorgesehenen Empfänger zu übertragen oder E-Mails in dienstliche und nicht dienstliche E-Mails klassifiziert bereitzustellen.

35

#### Aufgabe der Erfindung

- Aufgabe der vorliegenden Erfindung ist es, Lösungen bereitzustellen, die sicher verhindern, dass an einen  
40 Empfänger gerichtete Nachrichten diesem bereitgestellt

werden, wenn es sich dabei um unerwünschte Nachrichten handelt, wobei insbesondere die oben genannten Nachteile des Standes der Technik vermieden werden sollen.

## 5 Kurzbeschreibung der Erfindung

Im Folgenden sind Begriffe, die zur Definition und Beschreibung der vorliegenden Erfindung verwendet werden, beispielhaft und veranschaulichend erläutert:

10

Der erste Empfänger ist ein erstes eingerichtetes Benutzerkonto (User Account) in einem Kommunikationsdienst, wie z.B. Email, oder Mobilfunk, SMS (Short Message Service) oder MMS (Multi Media Message Service), an das auch solche  
15 Nachrichten gerichtet sein können, deren Absender und/oder Inhalt nicht bekannt sind und vor die der Benutzer des ersten Empfängers geschützt werden soll. Im bevorzugten Beispiel ist der erste Empfänger der Email-Account eines Kindes, das vor „unerwünschten“ und/oder „unbekannten“  
20 Nachrichten geschützt werden soll.

Der zweite Empfänger ist ein zweites eingerichtetes Benutzerkonto (User Account), von dem aus der Zugriff auf „unerwünschte“ und/oder „unbekannte“ Nachrichten durch den  
25 ersten Empfänger verhindert wird. Im bevorzugten Beispiel ist der zweite Empfänger der Email-Account eines Erziehungsberechtigten des Kindes (Eltern, Pädagogen usw.), der „unerwünschten“ und/oder „unbekannten“ Nachrichten, die an das Email-Postfach des Kindes gerichtet sind, überwachen  
30 kann und vor dem Zugriff durch das Kind sperren kann. Das Kind erhält vorzugsweise nur „erwünschte“ Nachrichten.

Die Nachrichten „unerwünscht“, „erwünscht“ und „unbekannt“ werden von jeweils einer entsprechend eingerichteten  
35 ersten, zweiten bzw. dritten Empfangsvorrichtung empfangen, die im Falle von Emails entsprechend eingerichtete Postfach-Ordner sind. Die eingehenden Nachrichten werden also kategorisiert und entsprechend der Kategorie einem ersten Ordner „Unerwünscht“ oder einem zweiten Ordner

„Erwünscht“ oder im Zweifelsfall einem dritten Ordner  
„Unbekannt“ zugeordnet.

Es wird auf Nachrichtenkategorien Bezug genommen, die als  
5 "unerwünscht", "erwünscht" und "unbekannt" bezeichnet  
werden. Die Nachrichtenkategorie "unerwünscht" gibt  
Nachrichten an, bei denen verhindert werden soll, dass sie  
einem Benutzer eines Empfängers bereitgestellt werden, der  
von einem Absender einer Nachricht als Empfänger vorgesehen  
10 ist. Die Nachrichtenkategorie "erwünscht" gibt Nachrichten  
an, die einem Empfänger bereitgestellt werden dürfen, der  
von einem Absender einer Nachricht als Empfänger vorgesehen  
ist. Die Nachrichtenkategorie "unbekannt" gibt Nachrichten  
an, die weder in die Nachrichtenkategorie "unerwünscht"  
15 noch in die Nachrichtenkategorie "erwünscht" fallen.  
Nachrichten der Nachrichtenkategorie "unbekannt" werden als  
solche gekennzeichnet und vorzugsweise wie Nachrichten der  
Nachrichtenkategorie "unerwünscht" behandelt.

20 Zur Klassifizierung von Nachrichten als "unerwünschte",  
"erwünschte" und "unbekannte" Nachrichten sind  
Filterverfahren und/oder -vorrichtungen vorgesehen.  
Bevorzugte Beispiele hierfür sind weiter unten aufgeführt.

25 Hinsichtlich der Begriffe "unerwünscht", "erwünscht" und  
"unbekannt" ist es bevorzugt, dass diese Begriffe nicht aus  
Sicht des Benutzers, an den Nachrichten adressiert sind,  
sondern (auch) aus Sicht einer Instanz zum Überprüfen von  
an den Benutzer des ersten Empfängers gerichteten  
30 Nachrichten verstanden werden. Bleibt man bei dem Beispiel  
von an einen Minderjährigen gesendeten Nachrichten, kann  
die Definition der Nachrichtenkategorie "unerwünscht" so  
erfolgen, dass sie nicht im Sinne des Minderjährigen  
erfolgt. Vielmehr ist es möglich, die Definition der  
35 Nachrichtenkategorie "unerwünscht" seitens Eltern,  
Aufsichtspersonen etc. festzulegen, um zu verhindern, dass  
Minderjährige aus Sicht solcher Personen unerwünschte  
Nachrichten erhalten. Entsprechendes gilt für die  
Nachrichtenkategorien "erwünscht" und "unbekannt".

Ferner wird auf das Bereitstellen einer Nachricht Bezug genommen. Darunter ist insbesondere zu verstehen, dass eine Nachricht einem Benutzer eines Empfängers so bereitgestellt wird, dass die Nachricht von dem Benutzer in der von dem Absender und/oder für die Nachricht selbst vorgesehenen Art und Weise verwendet werden kann. Beispielsweise wird eine E-Mail bereitgestellt, wenn der als Adressat genannte Benutzer auf die E-Mail zugreifen bzw. die E-Mail lesen, speichern usw. kann.

Beispiele für bei der vorliegenden Erfindung vorgesehene Empfänger umfassen zur Kommunikation über ein Netzwerk, insbesondere das Internet ausgelegte Rechnersysteme (z. B. Personalcomputer), E-Mail-Accounts etc. Wie im Folgenden ersichtlich kann der Begriff "Empfänger" Vorrichtungen oder Einrichtungen umfassen, die Nachrichten empfangen und versenden können ( in solchen Fällen kann der Begriff "Empfänger" als zur Abgrenzung gegenüber einem Absender einer Nachricht gewählt verstanden werden).

Bei der vorliegenden Erfindung vorgesehene Empfänger, für die eine Überprüfung von Nachrichten erfolgen soll, umfassen wenigstens eine Empfangseinrichtung. Beispiele für bei der vorliegenden Erfindung vorgesehene Empfangseinrichtungen umfassen einem Empfänger zugeordnete Speicherbereiche zur Speicherung von Nachrichten, sogenannte Ordner von E-Mail-Accounts und dergleichen.

Zur Lösung dieser Aufgabe stellt die vorliegende Erfindung ein Verfahren und ein System zur Nachrichtenüberwachung bereit.

Bei dem erfindungsgemäßen Verfahren werden an einen ersten Empfänger adressierte Nachrichten überwacht, indem der erste Empfänger so eingerichtet wird, dass er eine Empfangseinrichtung "unerwünscht" aufweist und dass Zugriffe eines Benutzers des ersten Empfängers auf die Empfangseinrichtung "unerwünscht" verhindert werden. Es wird eine Nachrichtenkategorie "unerwünscht" definiert, die Nachrichten angibt, für die verhindert werden soll, dass

sie einem Benutzer des ersten Empfängers bereitgestellt werden. Eine an den ersten Empfänger adressierte Nachricht wird dahingehend geprüft, ob sie in die Nachrichtenkategorie "unerwünscht" fällt. Die Nachricht  
5 wird dann der Empfangseinrichtung "unerwünscht" zugeordnet, wenn die Nachricht in die Nachrichtenkategorie "unerwünscht" fällt, wobei der erste Empfänger so eingerichtet wird, dass auf die Empfangseinrichtung "unerwünscht" nur durch einen zweiten Empfänger zugegriffen  
10 werden kann.

Dies ermöglicht die Verwendung und Definition einer Kontrollinstanz, die Nachrichten der Nachrichtenkategorie "unerwünscht" prüft. Beispielsweise kann der zweite  
15 Empfänger ein von Eltern genutzter Empfänger (z. B. ein E-Mail-Account) sein, mittels dem die Eltern für ihr Kind unerwünschte Nachrichten kontrollieren.

Auf diese Weise werden mehrere Probleme des Standes der  
20 Technik gelöst.

Beim Stand der Technik ist es möglich, dass ein Empfänger und damit dessen Benutzer an ihn gerichtete Nachrichten überhaupt nicht erhält, also Nachrichten verloren gehen,  
25 wenn Nachrichten (fälschlicherweise) als unerwünschte Nachrichten eingestuft und überhaupt nicht bereitgestellt werden. Dies wird durch die vorliegende Erfindung verhindert, weil Nachrichten, die nicht dem Benutzer des ersten Empfängers bereitgestellt werden sollen, von der  
30 Empfangseinrichtung "unerwünscht" empfangen werden, also nicht verloren gehen.

Ferner ist es beim Stand der Technik möglich, dass auf Nachrichten, die ein Benutzer eines Empfängers eigentlich  
35 nicht erhalten soll, zwar als solche Nachrichten gekennzeichnet werden (z. B. als unerwünschte angegebene oder einem speziellen Ordner zugeordnete Nachrichten), aber der Benutzer auf solche Nachrichten trotzdem zugreifen kann. Dies wird durch die vorliegende Erfindung verhindert, indem  
40 in die Nachrichtenkategorie "unerwünscht" fallende



Nachrichten der Empfangseinrichtung "unerwünscht" bereitgestellt werden, auf die der Benutzer des ersten Empfängers nicht zugreifen kann.

- 5 Auf diese Weise ist es beispielsweise möglich, an einen Minderjährigen adressierte E-Mails dahingehend zu überprüfen, ob sie unerwünschte Inhalte (z. B. pornographische Inhalte) aufweisen oder von unerwünschten Absendern (z. B. politische Gruppierungen, bestimmte  
10 Verwandte) stammen, d. h. in eine entsprechend definierte Nachrichtenkategorie "unerwünscht" fallen. In solchen Fällen werden an den Minderjährigen gerichtete E-Mails nicht diesem zur Nutzung (z. B. Lesen, Speichern und/oder Weiterleiten), sondern zugriffsgesichert von der  
15 Empfangseinrichtung "unerwünscht" aufgenommen und beispielsweise den Eltern zur Verfügung gestellt.

- Ein weiteres Beispiel ist ein dienstlich genutzter, erster Empfänger, dessen Benutzer keine private Nachrichten oder  
20 Nachrichten fremder Unternehmer erhalten soll; hierfür wird eine solche Nachrichten angehende Nachrichtenkategorie "unerwünscht" definiert. An den dienstlich genutzten, ersten Empfänger gerichtete Nachrichten werden hinsichtlich der Nachrichtenkategorie "unerwünscht" überprüft (z. B.  
25 stammt die Nachricht von einem privaten Absender) und gegebenenfalls einer entsprechenden Empfangseinrichtung "unerwünscht" bereitgestellt.

- Bei einer bevorzugten Ausführungsform wird der erste  
30 Empfänger so eingerichtet, dass er eine Empfangseinrichtung "erwünscht" aufweist und dass Zugriffe eines Benutzers des ersten Empfängers auf die Empfangseinrichtung "erwünscht" zugelassen werden. Es wird eine Nachrichtenkategorie "erwünscht" definiert, die Nachrichten angibt, die einem  
35 Benutzer des ersten Empfängers bereitgestellt werden. Die an den ersten Empfänger adressierte Nachricht wird überprüft, ob sie in die Nachrichtenkategorie "erwünscht" fällt. Wenn die Nachricht in die Nachrichtenkategorie "erwünscht" fällt, wird die Nachricht der  
40 Empfangseinrichtung "erwünscht" zugeordnet.

In Abhängigkeit der Nachrichtenkategorien kann es vorteilhaft sein, die Überprüfung, ob eine Nachricht in die Nachrichtenkategorie "erwünscht" fällt, vor der Überprüfung hinsichtlich der Nachrichtenkategorie "unerwünscht" durchzuführen. Resultiert beispielsweise die Nachrichtenkategorie "erwünscht" verglichen mit der Nachrichtenkategorie "unerwünscht" in einer geringeren Anzahl von Nachrichten, die bereitgestellt werden dürfen, kann die Überprüfung von Nachrichten hinsichtlich der Nachrichtenkategorie "erwünscht" schneller erfolgen. Umgekehrt kann es vorteilhaft sein, die Überprüfung hinsichtlich der Nachrichtenkategorie "unerwünscht" vor der Überprüfung hinsichtlich der Nachrichtenkategorie "erwünscht" durchzuführen, wenn beispielsweise die Nachrichtenkategorie "unerwünscht" schneller zu prüfen ist. Die Reihenfolge von Überprüfungen hinsichtlich der Nachrichtenkategorien kann auch für einzelne oder mehrere, beispielsweise gruppierte Nachrichten separat vorgegeben und/oder gesteuert werden.

Bei einer weiteren bevorzugten Ausführungsform wird der erste Empfänger so eingerichtet wird, dass er eine Empfangseinrichtung "unbekannt" aufweist und dass Zugriffe eines Benutzers des ersten Empfängers auf die Empfangseinrichtung "unbekannt" verhindert werden. Es wird eine Nachrichtenkategorie "unbekannt" definiert, die Nachrichten angibt, die nicht in die Nachrichtenkategorie "unerwünscht" und nicht in die Nachrichtenkategorie "erwünscht" fallen. Dann wird überprüft, ob die an den ersten Empfänger adressierte Nachricht in die Nachrichtenkategorie "unbekannt" fällt; trifft dies zu, wird die Nachricht der Empfangseinrichtung "unbekannt" zugeordnet.

Diese Ausführungsform vermeidet, dass Nachrichten, die beispielsweise durch eine geeignete Form versuchen, nicht in die Nachrichtenkategorie "unerwünscht" klassifiziert zu werden, obwohl sie eigentlich in diese fallen, von dem Benutzer des ersten Empfängers genutzt werden können.

Solche "undefinierbaren" oder "unbekannten" Nachrichten werden von der Empfangseinrichtung "unbekannt" empfangen, wo - wie unten ausgeführt - entschieden werden kann, ob solche Nachrichten dem Benutzer des ersten Empfängers  
5 bereitgestellt werden können.

Zur Definition der Nachrichtenkategorie(n) ist es beispielsweise vorgesehen, wenigstens eines der folgenden Kriterien, Parameter etc. zu verwenden:

10

- Absender von Nachrichten charakterisierende Angaben (z. B. E-Mail-Adresse, IP-Adressen, Telefonnummer, Absendername, postalische Absenderadresse)
- Nachrichteninhalte (z. B. durch Textanalysesoftware- und/oder  
15 -hardware, Sprachanalyse)
- Datum und/oder Uhrzeit für das Absenden von Nachrichten (z. B. Nachts an Minderjährige versendete Nachrichten, in der Mittagspause versendete Nachrichten für einen dienstlich genutzten ersten Empfänger)
- Datum und/oder Uhrzeit für den Eingang von Nachrichten (z. B. Nachts erhaltene Nachrichten an Minderjährige, in der Mittagspause eingegangene Nachrichten für einen dienstlich genutzten ersten Empfänger)
- zur Nachrichtenübertragung verwendete Systeme, Komponenten, Hard- und/oder Software etc. (z. B.  
25 unsichere Internet-Server, ausländische Telefonanschlüsse, private Telefonanschlüsse [wenn im dienstlichen Bereich die Übertragung privater Nachrichten verhindert werden soll], dienstliche und/oder amtliche  
30 Telefonanschlüsse [wenn im privaten Bereich die Übertragung dienstlicher oder amtlicher Nachrichten, z. B. von der Schule, verhindert werden soll])
- Nachrichtenart (um beispielsweise zu verhindern, dass unter Verwendung von E-Mails versendete Sprachnachrichten  
35 dem ersten Empfänger bereitgestellt werden)
- Nachrichtengröße (um beispielsweise zu gewährleisten, dass nur E-Mails bis zu einer vorgegebene Datenmenge dem ersten Empfänger bereitgestellt werden)
- Frequenz eingehender Nachrichten

40

Insbesondere ist es vorgesehen, zur Definition und Speicherung solcher Kriterien, Parameter etc. sogenannte Blacklists und Whitelists zu verwenden. Gemäß einer Blacklist können Nachrichten identifiziert werden, die in die Nachrichtenkategorie "unerwünscht" fallen, während anhand einer Whitelist Nachrichten der Nachrichtenkategorie "erwünscht" erkannt werden. Die Whitelist kann vorzugsweise anhand eines elektronischen Adressbuches (Datei und/oder Datenbank mit Kontaktdaten) erstellt werden, insbesondere durch ein Online-Adressbuch, das auf einem Server liegt und per Webzugang von einer berechtigten Person (User) genutzt werden kann. In dem Adressbuch sind die Kontaktdaten und Adressen, insbesondere Namen und Email-Adressen von Freunden und Bekannten, eingetragen, die zu den Kontakten gehören, die dem User bekannt und vertraut sind. Dadurch wird sichergestellt, dass nur solche Nachrichten als „erwünscht“ eingestuft werden, die von vertrauten Kontakten gesendet wurden. Das Adressbuch ist vorzugsweise nur für den Benutzer (User) des zweiten Empfängers (Eltern) und nicht oder nur eingeschränkt für den Benutzer des ersten Empfängers (Kind) zugänglich. Insbesondere können die Daten nur von dem ersten Empfänger aus (Eltern) eingetragen, geändert oder gelöscht werden. Das Kind hat allenfalls Leserechte. Für Nachrichten, die gemäß einer Blacklist und einer Whitelist weder in die Nachrichtenkategorie "Unerwünscht" noch in die Nachrichtenkategorie "erwünscht" fallen, können z. B. einer Inhaltskontrolle unterzogen werden, um festzustellen, in welche der Nachrichtenkategorie die betreffende Nachricht fällt.

Der erste Empfänger kann so eingerichtet werden, dass auf die Empfangseinrichtung "unerwünscht" nur durch einen zweiten Empfänger zugegriffen werden kann. Dies ermöglicht die Verwendung und Definition einer Kontrollinstanz, die Nachrichten der Nachrichtenkategorie "unerwünscht" prüft. Beispielsweise kann der zweite Empfänger ein von Eltern genutzter Empfänger (z. B. ein E-Mail-Account) sein, mittels dem die Eltern für ihr Kind unerwünschte Nachrichten kontrollieren. Mit anderen Worten: Der erste Empfänger kann ein E-Mail-Account eines Kindes sein und der

- zweite Empfänger kann ein E-Mail-Account eines Erwachsenen (Eltern, Erziehungsberechtigter usw.) sein, der verhindern kann, dass das Kind auf unerwünschte Nachrichten, insbesondere auf Spam, Zugriff hat. Die Empfangsvorrichtung
- 5 „unerwünscht“ ist dabei ein entsprechender Ordner „unerwünscht“ im Postfach des ersten Empfängers (Kind). Der erste Empfänger ist also zumindest beim Zugriff auf die Empfangsvorrichtung bzw. den Ordner „unerwünscht“ beschränkt durch den zweiten Empfänger. Der zweite
- 10 Empfänger (Eltern) ist quasi die Kontrollinstanz für unerwünschte Nachrichten, die an das Postfach des Kindes gerichtet sind und vor die das Kind geschützt werden soll. Zusätzlich oder alternativ zum Ordner „unerwünscht“ kann auch ein Ordner „unbekannt“ eingerichtet werden, in dem
- 15 eingehende und an das Kind gerichtete Nachrichten gesammelt werden, deren Absender und/oder Inhalt nicht klar ist, d.h. solche Nachrichten, die wahrscheinlich schädlich für das Kind sein dürften.
- 20 Vorzugsweise wird der erste Empfänger so eingerichtet, dass auf die Empfangseinrichtung „unbekannt“ nur durch den zweiten Empfänger zugegriffen werden kann. Dies ermöglicht die Verwendung und Definition einer Kontrollinstanz, die Nachrichten der Nachrichtenkategorie „unbekannt“ prüft.
- 25 Beispielsweise kann der zweite Empfänger ein von Eltern genutzter Empfänger (z. B. ein E-Mail-Account) sein, mittels dem die Eltern Nachrichten der Nachrichtenkategorie „unbekannt“ für ihr Kind kontrollieren.
- 30 Bei einer weiteren bevorzugten Ausführungsform wird der erste Empfänger so eingerichtet, dass Änderungen der Nachrichtenkategorie „unerwünscht“ durch den Benutzer des ersten Empfängers verhindert werden und die Definition der Nachrichtenkategorie „unerwünscht“ nur durch den zweiten
- 35 Empfänger durchgeführt werden kann. Auf diese Weise können Manipulationen verhindert werden, die es ermöglichen, dass Nachrichten dem ersten Empfänger bereitgestellt werden, für die dies verhindert werden soll.

- Vorzugsweise wird der erste Empfänger so eingerichtet, dass Änderungen der Nachrichtenkategorie "unbekannt" durch einen Benutzer des ersten Empfängers verhindert werden und die Definition der Nachrichtenkategorie "unbekannt" nur durch den zweiten Empfänger durchgeführt werden kann. Auf diese Weise können Manipulationen verhindert werden, die es ermöglichen, dass Nachrichten dem ersten Empfänger bereitgestellt werden, für die dies verhindert werden soll.
- 10 Ferner ist es vorgesehen, dass der Benutzer des ersten Empfängers die Nachrichtenkategorie "erwünscht" wenigstens teilweise definieren kann. Dies kann z. B. dadurch erfolgen, dass der Benutzer des ersten Empfängers eine Whitelist durch Angaben, insbesondere Namen, Adressen etc.
- 15 von Absendern erstellen und/oder ergänzen kann, von denen Nachrichten erwünscht sind. Dies kann indirekt Auswirkungen auf die Nachrichtenkategorie "unerwünscht" und, falls verwendet auf die Nachrichtenkategorie "unbekannt" haben. Um bei derartigen Ausführungsformen eine Umgehung der
- 20 Überprüfung von Nachrichten zu vermeiden, kann in solchen Fällen die Wirksamkeit einer Änderung durch den Benutzer des ersten Empfängers davon abhängig gemacht werden, ob der Benutzer des zweiten Empfängers der Änderung zustimmt.
- 25 Es können Nachrichten in der Empfangseinrichtung "unerwünscht" unter Verwendung des zweiten Empfängers bezüglich wenigstens eines Kriteriums, Parameters etc. (beispielsweise siehe oben) kontrolliert werden, um zu prüfen, ob die Nachrichten in der Empfangseinrichtung
- 30 "unerwünscht" nicht doch dem Benutzer des ersten Empfängers bereitgestellt werden können. Als Kriterien können z. B. einzelne, mehrere oder alle der oben aufgeführten oder weitere Kriterien herangezogen werden. Dies kann beispielsweise wünschenswert sein, um zu prüfen, ob eine
- 35 verwendete Blacklist zufriedenstellend definiert ist. Nachrichten, für die eine solche Kontrolle erfolgreich war, können dann unter Steuerung des zweiten Empfängers der Empfangseinrichtung "erwünscht" zugeordnet werden. Dort stehen sie dem Benutzer des ersten Empfängers wie
- 40 gewöhnliche Nachrichten der Nachrichtenkategorie

"erwünscht" zur Verfügung. Um dies in Zukunft zu vermeiden kann z. B. die verwendete Blacklist entsprechend überarbeitet werden.

- 5 Vergleichbar dazu können Nachrichten der  
Empfangseinrichtung "unbekannt" unter Verwendung des  
zweiten Empfängers bezüglich wenigstens eines Kriteriums,  
Parameters etc. (beispielsweise siehe oben) kontrolliert  
werden, um zu prüfen, ob die Nachrichten in der  
10 Empfangseinrichtung "unbekannt" nicht doch dem Benutzer des  
ersten Empfängers bereitgestellt werden können. Als  
Kriterien können z. B. einzelne, mehrere oder alle der oben  
aufgeführten oder weitere Kriterien herangezogen werden.  
Nachrichten, für die eine solche Kontrolle erfolgreich war,  
15 können dann unter Steuerung des zweiten Empfängers der  
Empfangseinrichtung "erwünscht" zugeordnet werden. Dort  
stehen sie dem Benutzer des ersten Empfängers wie  
gewöhnliche Nachrichten der Nachrichtenkategorie  
"erwünscht" zur Verfügung.

- 20 Bei weiteren bevorzugten Ausführungsformen kann als erster  
Empfänger ein erster E-Mail-Account verwendet werden, dem  
ein Ordner "Unerwünscht" zum Bereitstellen von Nachrichten  
der Nachrichtenkategorie "unerwünscht" und/oder ein Ordner  
25 "Erwünscht" zum Bereitstellen von Nachrichten der  
Nachrichtenkategorie "erwünscht" und/oder ein Ordner  
"Unbekannt" zum Bereitstellen von Nachrichten der  
Nachrichtenkategorie "unbekannt" zugeordnet ist.

- 30 Des weiteren ist es bevorzugt, dass - unabhängig von der  
Art des ersten Empfängers- als zweiter Empfänger ein E-  
Mail-Account verwendet wird.

- Die Überprüfung der an den ersten Empfänger adressierten  
35 Nachricht kann vor einer Übertragung zu dem ersten  
Empfänger z. B. durch eine zur Nachrichtenübertragung  
verwendeten Vorrichtung (z. B. ein E-Mail-Server)  
durchgeführt werden.

Um zu überprüfen, in welche Nachrichtenkatgorie die an den ersten Empfänger adressierte Nachricht fällt, kann eine Wahrscheinlichkeit ermittelt werden, die angibt, ob die Nachricht in die Nachrichtenkatgorie "unerwünscht" und/oder "erwünscht" und/oder "unbekannt" fällt.

Insbesondere ist es vorgesehen, zum Überprüfen der Nachricht einen Filter zu verwenden, der Nachrichten für den ersten Empfänger in die Nachrichtenkatgorien klassifiziert. In Anlehnung an bei herkömmlichen E-Mail-Systemen verwendeten Ansätzen, kann der bei der vorliegenden Erfindung vorgesehene Filter als Spamfilter bezeichnet werden.

Vorzugsweise wird ein Filter verwendet, der wie folgt arbeitet:

Für jede Nachricht wird überprüft, ob es sich um eine erwünschte Nachricht handelt. Beispielsweise werden Information verwendet, die Beziehungen zwischen dem zum Empfang der Nachricht vorgesehenen ersten Empfänger und einem Absender der Nachricht so charakterisieren, so dass Nachrichten, die im Einklang mit diesen Informationen stehen, eindeutig als erwünschte Nachrichten identifiziert werden können; es kann also eine Wahrscheinlichkeit von z. B. 0 % definiert werden, dass es sich dabei um eine unerwünschte Nachricht (z. B. Spam) handelt.

Beispiele für solche Informationen umfassen Nachrichten von Absendern, die im Adressbuch des ersten Empfängers eingetragen sind, Nachrichten von Absender, für die der Benutzer des ersten Empfängers definiert hat, dass Nachrichten von diesen Absender immer erwünschte Nachrichten sind, und Nachrichten, die speziell für den Benutzer des ersten Empfängers verschlüsselt, codiert oder auf andere Weise gekennzeichnet sind.

Um solche Informationen zu speichern und zu verwalten, kann eine sogenannte Whitelist verwendet werden.



Ferner wird beurteilt, ob Nachrichten vorliegen, bei denen es sich wahrscheinlich nicht um unerwünschte Nachrichten (z. B. Spam) handelt, weil beispielsweise eine positive Aussage über den Absender getroffen werden kann (z. B. weil  
5 der Absender als vertrauenswürdig bekannt ist). In diesen Fällen kann eine geringe Wahrscheinlichkeit von z. B. 1 % definiert werden, dass es sich bei solchen Nachrichten um unerwünschte Nachrichten (z. B. Spam) handelt. Beispiele für hierbei verwendbare Kriterien umfassen Nachrichten,  
10 deren Absender eindeutig identifizierbar ist, Nachrichten von bezahlenden Kunden des Serverbetreibers, Nachrichten von sehr aktiven Kunden des Serverbetreibers, Nachrichten, die mit dem Frontend des Serverbetreibers erstellt wurden, Nachrichten, die von Absendern aus einer vom Benutzer  
15 freigegebenen Maildomain stammen, Nachrichten, die mit digitalen Unterschriften versehen sind, und Nachrichten, die mit digitalen Unterschriften versehen sind, deren Vertrauenswürdigkeit jeweils mittels einem von einer Zertifizierungsstelle erstellten Zertifikat gesichert ist.

20 Des weiteren wird ermittelt, bei welchen Nachrichten es sich um unerwünschte Nachrichten (z. B. Spam) handelt. Dabei können Verfahren, wie z.B. Frequenzmessung, Inhaltsanalyse, Headeranalyse, verwendet werden.

25 In Abhängigkeit der Sicherheit, mit der unerwünschte Nachrichten (z. B. Spam) erkannt werden kann, kann eine Wahrscheinlichkeit definiert werden, dass es sich bei einer überprüften Nachricht um eine unerwünschte Nachricht (z.  
30 B. SPAM) handelt. Ist beispielsweise bekannt, dass Nachrichten von einem speziellen Absender unerwünscht sind, kann eine Wahrscheinlichkeit von z. B. 100 % definiert werden, dass es sich bei diesen Nachrichten um unerwünschte Nachrichten (z. B. Spam) handelt.

35 Für Nachrichten, für nicht mit Sicherheit ermittelt werden kann, ob es sich um erwünschte oder unerwünschte Nachrichten handelt, kann eine Wahrscheinlichkeit von z. B. 50 % oder ein Wahrscheinlichkeitsbereich von 1 % bis 90 %

definiert werden. Solche Nachrichten können in die Nachrichtenkategorie "unbekannt" eingeordnet werden.

Aufgrund der Identifikation der Nachrichten als erwünschte  
5 Nachrichten, unerwünschte Nachrichten und unbekannte  
Nachrichten, die nicht sicher als erwünscht oder  
unerwünscht erkannt wurden, werden die Nachrichten den  
Empfangseinrichtungen "unerwünscht", "erwünscht" bzw.  
"unbekannt" zugeordnet; bei Verwendung von Ordnern eines E-  
10 Mail-Accounts werden die klassifizierten Nachrichten in die  
Ordner "Unerwünscht", "Erwünscht" bzw. "Unbekannt"  
verteilt.

So können der Empfangseinrichtung "erwünscht" (Ordner  
15 "Erwünscht") nur Nachrichten zugeordnet werden, die mit  
hoher Wahrscheinlichkeit keine unerwünschten Nachrichten  
sind, wenn beispielsweise eine Wahrscheinlichkeit gleich  
oder kleiner als 1 % vorliegt, dass es sich bei der  
Nachricht um eine unerwünschte Nachricht handelt.

20 Der Empfangseinrichtung "unerwünscht" (Ordner  
"Unerwünscht") können Nachrichten zugeordnet werden, die  
mit hoher Wahrscheinlichkeit unerwünschte Nachrichten sind,  
wenn beispielsweise eine Wahrscheinlichkeit gleich oder  
25 größer als 90 % vorliegt, dass es sich bei der Nachricht um  
eine unerwünschte Nachricht handelt.

Der Empfangseinrichtung "unbekannt" (Ordner "Unbekannt")  
können Nachrichten zugeordnet werden, die weder "eindeutig"  
30 als erwünschte Nachrichten noch "eindeutig" als  
unerwünschte Nachrichten erkannt werden, wenn  
beispielsweise eine Wahrscheinlichkeit zwischen 1 % und 90  
% vorliegt, dass es sich bei der Nachricht um eine  
unerwünschte Nachricht handelt.

35 Aufgrund der Funktion des zweiten Empfängers, Nachrichten  
an den ersten Empfänger zu überwachen, können der zweite  
Empfänger als übergeordneter Empfänger oder Master-  
Empfänger und der erste Empfänger als untergeordneter

Empfänger oder Slave-Empfänger bezeichnet werden (z. B. im Fall von E-Mails als Master-Account und als Slave-Account).

Die Sicherheit kann dadurch erhöht werden, dass es dem  
5 zweiten Empfänger ermöglicht wird, auf dem ersten Empfänger bereitgestellte erwünschte Nachrichten zuzugreifen, vorteilhafterweise unabhängig von den entsprechenden Überprüfungsergebnissen. Auf diese Weise kann  
beispielsweise überprüft werden, ob die bei der Definition  
10 der Nachrichtenkategorie "unerwünscht" herangezogen Kriterien geändert, ergänzt oder modifiziert werden müssen. Auch lässt sich auf diese Weise feststellen, ob es möglich ist, die Überprüfung von an den ersten Empfänger versandte Nachrichten zu umgehen.

15 Die vorliegende Erfindung stellt ferner ein System zur Überwachung von Nachrichten bereit, das einen ersten Empfänger, der eine Empfangseinrichtung "unerwünscht" aufweist und so eingerichtet ist, dass Zugriffe eines  
20 Benutzers des ersten Empfängers auf die Empfangseinrichtung "unerwünscht" verhindert werden, einen zweiten Empfänger zum Definieren einer Nachrichtenkategorie "unerwünscht", die Nachrichten angibt, für die verhindert werden soll, dass sie einem Benutzer des ersten Empfängers  
25 bereitgestellt werden, und eine Einrichtung umfasst, um zu überprüfen, ob eine an den ersten Empfänger adressierte Nachricht in die Nachrichtenkategorie "unerwünscht" fällt, und um die Nachricht der Empfangseinrichtung "unerwünscht" zuzuordnen, wenn die Nachricht in die Nachrichtenkategorie  
30 "unerwünscht" fällt.

Vorzugsweise weist der erste Empfänger eine Empfangseinrichtung "erwünscht" auf und ist so eingerichtet, dass Zugriffe eines Benutzers des ersten  
35 Empfängers auf die Empfangseinrichtung "erwünscht" zugelassen werden, wobei der zweite Empfänger eingerichtet ist, um eine Nachrichtenkategorie "erwünscht" zu definieren, die Nachrichten angibt, die einem Benutzer des ersten Empfängers bereitgestellt werden sollen. Hier ist  
40 die Überprüfungseinrichtung eingerichtet, um zu überprüfen,

ob die an den ersten Empfänger adressierte Nachricht in die Nachrichtenkategorie "erwünscht" fällt, und um die Nachricht der Empfangseinrichtung "erwünscht" zuzuordnen, wenn die Nachricht in die Nachrichtenkategorie "erwünscht" fällt.

Bei einer weiteren bevorzugten Ausführungsform weist der erste Empfänger eine Empfangseinrichtung "unbekannt" auf und ist so eingerichtet, dass Zugriffe eines Benutzers des ersten Empfängers auf die Empfangseinrichtung "unbekannt" verhindert werden, wobei der zweite Empfänger zum Definieren einer Nachrichtenkategorie "unbekannt" eingerichtet ist, die Nachrichten angibt, die nicht in die Nachrichtenkategorie "unerwünscht" und nicht in die Nachrichtenkategorie "erwünscht" fallen. Hier ist die Überprüfungseinrichtung eingerichtet, um zu überprüfen, ob die an den ersten Empfänger adressierte Nachricht in die Nachrichtenkategorie "unbekannt" fällt, und um die Nachricht der Empfangseinrichtung "unbekannt" zuzuordnen, wenn die Nachricht in die Nachrichtenkategorie "unbekannt" fällt.

Vorzugsweise ist der erste Empfänger eingerichtet, dass auf die Empfangseinrichtung "unerwünscht" und/oder Empfangseinrichtung "unbekannt" nur durch den zweiten Empfängers zugegriffen werden kann.

Der zweite Empfänger kann eingerichtet sein, um die Empfangseinrichtung "unerwünscht" und/oder Empfangseinrichtung "unbekannt" zu kontrollieren und, falls gewünscht, kontrollierte Nachrichten der Empfangseinrichtung "erwünscht" zuzuordnen, auf die der erste Empfänger zugreifen kann.

Bei bevorzugten Ausführungsformen ist der erster Empfänger ein erster E-Mail-Account, dem wenigstens ein Ordner "Unerwünscht" zugeordnet ist, der als Empfangseinrichtung "unerwünscht" dient.

Bei Verwendung einer Nachrichtenkategorie "erwünscht" und/oder einer Nachrichtenkategorie "unbekannt", kann der erste E-Mail-Account einen als Empfangseinrichtung "erwünscht" dienenden Ordner "Erwünscht" bzw. einen als  
5 Empfangseinrichtung "unbekannt" dienenden Ordner "Unbekannt" aufweisen.

Vorzugsweise ist der zweite Empfänger (auch) ein E-Mail-Account.

10

Die Überprüfungseinrichtung kann einen Filter umfassen, der die an den ersten Empfänger adressierte Nachricht in Nachrichtenkategorie "unerwünscht" kategorisiert, wenn die Nachricht in die Nachrichtenkategorie "unerwünscht" fällt.

15

Die Überprüfungseinrichtung kann auch einen Filter umfassen, der die an den ersten Empfänger adressierte Nachricht in Nachrichtenkategorie "erwünscht" kategorisiert, wenn die Nachricht in die

20

Nachrichtenkategorie "erwünscht" fällt.

Ferner kann die Überprüfungseinrichtung einen Filter umfassen, der die an den ersten Empfänger adressierte Nachricht in Nachrichtenkategorie "unbekannt"

25

kategorisiert, wenn die Nachricht in die Nachrichtenkategorie "unbekannt" fällt.

Vorzugsweise ist der bzw. die Filter durch eine mit einem Spamfilter vergleichbare Vorrichtung bereitgestellt, die  
30 von dem ersten Empfänger umfasst oder eine Komponente einer Vorrichtung sein kann, die Nachrichten zu dem ersten Empfänger übermittelt und/oder beim ersten Empfänger zum Nachrichtenempfang verwendet wird, wie zum Beispiel E-Mail-Server, E-Mail-Browser etc.

35

Des weiteren ist es bevorzugt, dass bei der Filterung von Nachrichten an den ersten Empfänger eine oder mehrere Wahrscheinlichkeiten berechnet werden, dass eine Nachricht eine der Nachrichtenkategorien fällt.

40

### Kurzbeschreibung der Figuren

In der folgenden Beschreibung bevorzugter Ausführungsformen wird auf die beigefügten Figuren Bezug genommen, von denen  
5    zeigen:

Fig. 1 bis 11    schematische Darstellungen grafischer  
                  Benutzerschnittstellen für eine  
                  Ausführungsform des erfindungsgemäßen  
10                Verfahrens und

Fig. 12           eine schematische Darstellung einer  
                  Ausführungsform des erfindungsgemäßen  
                  Systems.

15

### Beschreibung bevorzugter Ausführungsformen

Im Folgenden wird unter Bezugnahme auf Fig. 1 bis 11 eine bevorzugte Ausführungsform beschrieben, bei der für als  
20   Kinderschutz-Accounts bezeichnete erste Empfänger Nachrichten in Form von E-Mails mittels als Kinderschutz bezeichneter Maßnahmen dahingehend überprüft werden, ob Nachrichten einem Kinderschutz-Account bereitgestellt werden sollen. Als zweiter Empfänger wird hierbei ein  
25   sogenannter Eltern-Account verwendet.

Hierbei wird ein normaler E-Mail-Account zu Grunde gelegt, dem drei Ordner zugeordnet sind, in denen E-Mail bereitgestellt werden können. Die drei Ordner werden als  
30   Ordner "Unerwünscht" für in die Nachrichtenkategorie "unerwünscht" fallende E-Mails, Ordner "Erwünscht" für in die Nachrichtenkategorie "erwünscht" fallende E-Mails und Ordner "Unbekannt" für in die Nachrichtenkategorie "unbekannt" fallende E-Mails bezeichnet. Ein Eltern-Account  
35   ist ein solcher normaler E-Mail-Account.

Der Kinderschutz-Account unterscheidet sich unter anderem in folgenden Punkten von einem normalen E-Mail-Account. Zu jedem Kinderschutz-Account gibt es genau einen Eltern-  
40   Account. In Kinderschutz-Accounts sind nur bestimmte E-

Mail-Funktionen verfügbar. Die Ordner "Unerwünscht" und "Unbekannt" sind nur über den Eltern-Account erreichbar (z. B. lesen, löschen, kopieren, weiterleiten etc.) und sind im Kinderschutz-Account nicht sichtbar. Der Ordner "Erwünscht" steht nur im Kinderschutz-Account zur Verfügung; ein Zugriff auf diesen Ordner über den Eltern-Account ist im Allgemeinen nicht möglich, um die Privatsphäre des Kindes zu schützen. Es ist aber möglich, auch einen Zugriff auf den Ordner "Erwünscht" über den Eltern-Account zu ermöglichen, um eine vollständige Kontrolle des Kommunikationsverhaltens des Kindes zu erreichen; eine solche Zugriffsmöglichkeit erlaubt auch zu prüfen, ob die zur Bewertung von an das Kind adressierten E-Mails verwendeten Kriterien (z. B. Filterparameter, Blacklist- und Whitelist-Einträge) so definiert sind, dass das Kind wirklich nur erwünschte E-Mails erhält. Wird bei einer Überprüfung des Ordners "Erwünscht" festgestellt, dass dort unerwünschte und/oder unbekannte E-Mails vorliegen, lässt dies auf eine nicht zufriedenstellende Überwachung bzw. unzureichende Kriterien und/oder auf von E-Mail-Absendern oder dem Kind genutzte Umgehungsmöglichkeiten schließen.

Ferner soll es bei einem Kinderschutz-Account nicht möglich sein, Spam-Schutz- bzw. -Filter zu deaktivieren, die Ordner "Unbekannt" und "Unerwünscht" anzuzeigen, das E-Mail-Postfachs vollständig zu löschen und das Geburtsdatum zu ändern, um die unten beschrieben altersabhängige Deaktivierung des Kinderschutzes zu manipulieren.

Auf der in Fig. 1 gezeigten Startseite im Eltern-Account findet sich unter der Rubrik "Posteingang" ein Link zum Kinderschutz. Durch Klick auf diesen Link gelangt man auf die in Fig. 2 veranschaulichte Seite "Kinderschutz verwalten". Die Seite "Kinderschutz verwalten" ist im Wesentlichen in drei Bereiche unterteilt.

Im oberen als "Aktivierte Kinderschutzkonten" bezeichneten Bereich befindet sich eine Übersicht über die bereits aktivierten Kinderschutz-Accounts, die dem Eltern-Account

zugeordnet sind. Dabei handelt es sich um eingerichtete und aktivierte Kinderschutz-Accounts.

Vom Eltern-Account aus hat man jeweils Zugriff auf die  
5 Ordner "Unbekannt" und "Unerwünscht" der Kinderschutz-Accounts und kann diese bearbeiten. Außerdem kann man von hier aus die einzelnen Kinderschutz-Accounts wieder deaktivieren. Nach der Deaktivierung wird aus einem Kinderschutz-Account wieder ein normaler E-Mail-Account.

10 Im unteren als "Neuen Kinderschutz einrichten" bezeichneten Bereich können weitere Kinderschutz-Accounts eingerichtet werden. Dazu ist einfach der Benutzername des gewünschten Accounts einzugeben. Weitere Angaben hierzu finden sich  
15 weiter unten.

Der mittlere als "Noch nicht aktivierte Kinderschutz-Konten" bezeichnete Bereich stellt die eingerichteten, aber noch nicht aktivierten Kinderschutz-Accounts dar. Aktiviert  
20 ist ein Kinderschutz-Account erst dann, wenn dort, wie im Folgenden beschrieben, ein Aktivatorkey eingegeben wird. Bis dahin können eingerichtete, aber noch nicht aktivierte Kinderschutz-Accounts wieder gelöscht werden.

25 Die Löschung eines noch nicht aktivierten Kinderschutzes ist darüber hinaus Voraussetzung dafür, dass für das betreffende Postfach erneut ein Kinderschutz eingerichtet werden kann.

30 Nach Eingabe des Namens eines E-Mail-Postfaches im Bereich "Neuen Kinderschutz einrichten" auf der Seite "Kinderschutz Verwalten" von Fig. 2 und bei Erfüllung aller notwendigen Voraussetzungen (Alter des Zielpostfach-Inhabers etc.) erscheint eine in Fig. 3 veranschaulichte Seite  
35 "Kinderschutz einrichten" des Eltern-Accounts. Dort werden weitere Schritte zur Aktivierung des Kinderschutz-Accounts erläutert.

Falls für ein älter als 17 Jahre altes Kind ein  
40 Kinderschutz-Account eingerichtet werden soll, wird nach



Betätigung des Schaltfeldes "einrichten" (siehe Fig. 2: Bereich "Neuen Kinderschutz einrichten") eine in Fig. 4 gezeigte Hinweisseite angezeigt. Diese enthält auch die Information darüber, wo das Geburtsdatum geändert werden  
5 kann. Das System blockiert also in Abhängigkeit vom Alter des Benutzers (Kind) des ersten Empfängers (Kinder-Account) bei Erreichen eines vorgebbaren Mindestalters (z.B. 17 Jahre) das Einrichten eines solchen Kinder-Accounts und damit die Kontrolle durch einen Eltern-Account. Damit wird  
10 vermieden, dass bei älteren Kinder, die bald volljährig sind, noch Kinder-Accounts eingerichtet werden können, die aus rechtlichen Gründen dann kurze Zeit später bei Erreichen der Volljährigkeit wieder aufgelöst oder in normale Accounts umgewandelt werden müssen.

15 Besteht aber bereits ein Kinder-Account und erreicht ein Kind, für dessen Account ein Kinderschutz aktiviert ist, das entsprechende Alter der Volljährigkeit (z.B. 18 Jahre), dann erhalten sowohl die Eltern als auch das Kind eine  
20 Benachrichtigung mit dem Inhalt, dass der Kinderschutz deaktiviert wird. Der Kinderschutz wird dann automatisch aufgehoben, wobei der Kinderschutz-Account und der Eltern-Account jeweils in normale Accounts umgewandelt werden. Die bis dahin bestandene Bindung bzw. Abhängigkeit des Kinder-Accounts vom Eltern-Account wird automatisch bei Erreichen  
25 eines Mindestalters, das die Volljährigkeit des Kindes angibt, aufgelöst. Diese Benachrichtigung kann per E-Mail erfolgen, die die Eltern und das Kind beim nächsten Login in den ehemaligen Eltern-Account bzw. den ehemaligen  
30 Kinderschutz-Account in den entsprechenden Ordnern "Erwünscht" vorfinden.

Ausgehend vom Eltern-Account, wenn man auf der Seite "Kinder-Schutz Verwalten" einen Ordnerlink eines  
35 Kinderschutz-Accounts wählt, gelangt man zu der in Fig. 5 dargestellten als "Ordnerübersicht" bezeichneten Seite. Die Seite "Ordnerübersicht" wird in anderen Farben dargestellt (z. B. grün), um eine zusätzliche Abgrenzung zum Posteingang des Eltern-Accounts zu erreichen.

40

Damit der Inhaber eines Eltern-Accounts Zugriff auf E-Mails von Kinderschutz-Accounts hat, ist es vorteilhaft, wenn die Postfächer der Eltern- und Kinderschutz-Accounts in einer Datenbank verwaltet werden, um bei einem von einem Eltern-  
5 Account ausgehenden Zugriff auf E-Mails eines Kinderschutz-Accounts Datenübertragungen zu vermeiden.

Hier hat man die Möglichkeit, einzelne E-Mails in dem entsprechenden Kinderschutz-Account als "Erwünscht" bzw.  
10 "Unerwünscht" zu markieren, indem die Schaltflächen "Mein Kind davor schützen" für unerwünschte E-Mails oder "Meinem Kind zeigen" für erwünschte E-Mails betätigt werden. Auf diese Weise können die Eltern beeinflussen, welche E-Mails im Posteingang des Kinderschutz-Accounts landen und somit,  
15 welche E-Mails das Kind zu sehen bekommt. Wenn eine E-Mail auf diese Weise als erwünscht markiert wird, wird die entsprechende E-Mail in den Posteingang verschoben; für den Absender einer solchen E-Mail kann ein Eintrag als  
"erwünschter Absender" generiert werden. Falls eine E-Mail  
20 als unerwünscht markiert wird, wird ein sogenannter Blacklist-Eintrag generiert.

Da der Inhaber des Eltern-Accounts keinen Zugriff auf Posteingänge von Kinderschutz-Accounts hat, wird der  
25 Posteingang des hier gewählten Kinderschutz-Accounts in einer dieses Zugriffsverbot angehenden Weise dargestellt.

Wenn ausgehend von der Seite "Ordnerübersicht" eine unter der Kategorie "Unbekannt" oder "Unerwünscht" angegebene E-Mail geöffnet wird, wird die in Fig. 6 dargestellte Seite  
30 "E-Mail lesen" dargestellt. Über die hier gezeigten Schaltflächen "Mein Kind davor schützen" und "Meinem Kind zeigen" können die Funktionalitäten der oben beschriebenen gleichnamigen Schaltflächen aktiviert werden. Eine  
35 Betätigung der Schaltfläche "Entfernen" bewirkt, dass die angezeigte E-Mail endgültig gelöscht wird.

Um ein Kinderschutz-Account zu deaktivieren, d.h. das betreffende Konto wieder zu einem normalen E-Mail-Account  
40 werden zu lassen, und um die Bindung zwischen Eltern- und

- Kinderschutz-Account zu lösen, gibt es zu jedem aktivierten Kinderschutz-Account auf der in Fig. 2 dargestellten Seite "Kinder-Schutz Verwalten" die Schaltfläche "Deaktivieren". Wird diese betätigt, gelangt man zu der in Fig. 7
- 5 dargestellten Seite "Kinder-Schutz deaktivieren". Dort kann die Deaktivierung abgebrochen oder tatsächlich ausgeführt werden, wobei auf die Konsequenzen einer Deaktivierung hingewiesen wird.
- 10 Die in Fig. 8 dargestellte Startseite eines Kinderschutz-Accounts unterscheidet sich aufgrund eingeschränkter Funktionalitäten eines Kinderschutz-Accounts von der in Fig. 1 dargestellten Startseite eines Eltern-Accounts.
- 15 Um Missbrauch bei der Einrichtung von Kinderschutz-Accounts vorzubeugen, wird nach dem oben beschriebenen Einrichten eines Kinderschutz-Accounts ausgehend von einem Eltern-Account eine E-Mail an den Account gesendet, der zu einem Kinderschutz-Account werden soll. Eine solche E-Mail stellt
- 20 einen Link bereit, mittels dem man zu der in Fig. 9 dargestellten Seite "Kinder-Schutz aktivieren" gelangt. Dort wird der zuvor generierte Aktivatorkey eingegeben werden, über den nur der Inhaber des Eltern-Accounts verfügt.
- 25 Nach erfolgreich abgeschlossenem Aktivierungsvorgang erscheint die in Fig. 10 dargestellte Seite. Hier erfolgt der Hinweis, dass der Aktivierungsvorgang beispielsweise in etwa einer Stunde abgeschlossen ist.
- 30 Wenn von einem Eltern-Account Kinderschutz deaktiviert wird, findet das Kind bei nächsten Login in seinem Ordner "Erwünscht" eine entsprechende E-Mail vor. Wenn bei einem Kinderschutz-Account wegen zu hohen Alters des Inhabers der
- 35 Kinderschutz deaktiviert wird, erhält dieser Informationen darüber ebenfalls per E-Mail und/oder über die in Fig. 11 gezeigte Seite.
- Eine Deaktivierung eines Kinderschutz-Accounts hat in allen
- 40 Fällen zu Folge, dass der Kinderschutz-Account in einen

herkömmlichen Account umgewandelt wird. Dem Benutzer des ehemaligen Kinderschutz-Accounts stehen dann alle üblichen Funktion eines normalen Accounts zur Verfügung ; insbesondere hat der Benutzer Zugriff auf die Ordner

5 "Unerwünscht", "Unbekannt" und "Erwünscht".

Fig. 12 veranschaulicht schematisch eine weitere Ausführungsform mit einem Kommunikationsnetzwerk N (z. B. das Internet), in dem ein Absender (nicht gezeigt) eine

10 Nachricht M zu einem Benutzer (nicht gezeigt) eines ersten Empfängers E1 senden möchte. Die Übertragung der Nachricht in dem Netzwerk N erfolgt unter Steuerung einer zentralen Vorrichtung S (z. B. E-Mail-Server) und gegebenenfalls von - hier nicht gezeigten - der Vorrichtung S zugeordneten

15 Vorrichtungen und/oder Einrichtungen (z. B. Gateways, Router, Netzwerkbetreiber etc.).

Um anzugeben, dass die Nachricht M an den ersten Empfänger E1 gerichtet ist, sind der Nachricht M Daten zugeordnet,

20 die den ersten Empfänger E1 als Adressaten angeben (z. B. E-Mail-Adresse). Die Vorrichtung S (bzw. damit verwendete Nachrichtenübermittlungsvor- und/oder -einrichtungen) erkennt anhand solcher Adressdaten, dass die Nachricht M zu dem ersten Empfänger E1 übertragen werden soll.

25 Anhand der Adressdaten wird auch festgestellt, ob die an den ersten Empfänger E1 gerichtete Nachricht M dahingehend überwacht werden soll, in welche Nachrichtenkatgorie die Nachricht M fällt.

30 Soll eine Überwachung der bei der zentralen Vorrichtung S eingegangenen Nachricht M erfolgen, wird die Nachricht M zu einer Überwachungseinrichtung Ü weitergeleitet (Schritt [2]). Bei der dargestellten Ausführungsform ist die

35 Überwachungseinrichtungen Ü der zentralen Vorrichtung S zugeordnet oder in diese integriert. Alternativ ist es möglich, die Überwachungseinrichtung Ü dem ersten Empfänger E1 zuzuordnen oder in diesen zu integrieren.

Die erhaltene Nachricht M wird von der Überwachungseinrichtung Ü dahingehend klassifiziert, in welche Nachrichtenkatgorie die Nachricht M fällt. Vorteilhafterweise ist die Überwachungseinrichtung Ü so  
5 eingerichtet, dass zur Klassifizierung der Nachricht M Wahrscheinlichkeiten berechnet werden, mit der die Nachricht M in eine der Nachrichtenkatgorien fällt.

Hierfür können eine sogenannte Blacklist und eine  
10 sogenannte Whitelist verwendet werden. Solche Listen können in dem ersten Empfänger E1 zugeordneter Weise in einem Speicherbereich der zentralen Vorrichtungen S vorliegen.

In der Blacklist sind Informationen angegeben, anhand derer es (eindeutig) möglich ist, Nachrichten als erwünschte  
15 Nachrichten zu identifizieren. Im Gegensatz dazu sind in der Whitelist Informationen vorhanden, die eine (eindeutige) Identifizierung von Nachrichten als unerwünschte Nachrichten ermöglichen. Anhand der Blacklist  
20 und der Whitelist und gegebenenfalls unter Verwendung weiterer Verfahren zur Bewertung von Nachrichten (z. B. Inhaltsanalyse, Headeranalyse etc.) können für Nachrichten Wahrscheinlichkeiten berechnet werden, ob Nachrichten in die Nachrichtenkatgorie "unerwünscht", in die  
25 Nachrichtenkatgorie "erwünscht" oder in die Nachrichtenkatgorie "unbekannt" fallen.

Stellt die Überwachungseinrichtung Ü fest, dass die Nachricht M in die Nachrichtenkatgorie "erwünscht" fällt,  
30 wird die Nachricht M zu der Empfangseinrichtung ERW ("erwünscht") übertragen (Schritt [4]).

Stellt die Übertragungseinrichtung Ü fest, dass die Nachricht M in die Nachrichtenkatgorie "unbekannt" fällt,  
35 erfolgt eine Zuordnung zu der Empfangseinrichtung UNB ("unbekannt") (Schritt [6]).

Ergibt in die Überprüfung der Nachricht M durch die Überprüfungseinrichtung Ü, dass die Nachricht M in die  
40 Nachrichtenkatgorie "unerwünscht" fällt, erhält die

Empfangseinrichtung UNE ("unerwünscht") die Nachricht M (Schritt [8]).

- 5 Auf die Empfangseinrichtung UNE und die Empfangseinrichtung UNB kann ein Benutzer des ersten Empfängers E1 nicht zugreifen; Zugriffe auf die Empfangseinrichtung ERW sind für den Benutzer der ersten Empfangseinrichtung E1 möglich. Dies ist in Fig. 12 durch die gestrichelte Linie veranschaulicht. Demgegenüber sind Zugriffe seitens des
- 10 Benutzers des zweiten Empfängers E2 auf die Empfangseinrichtung UNB und die Empfangseinrichtung UNE möglich, während Zugriffe auf die Empfangseinrichtung ERW im Allgemeinen nicht möglich sind.
- 15 Möchte der Benutzer des zweiten Empfängers E2 Nachrichten der Empfangseinrichtung UNE überprüfen, greift er auf diese Empfangseinrichtung zu (Schritt [10]). Dies ermöglicht es dem Benutzer des zweiten Empfängers E2 unerwünschte Nachrichten zu löschen. Ferner kann der Benutzer des
- 20 zweiten Empfängers E2 unerwünschte Nachrichten nochmals prüfen, ob trotz der Klassifizierung in die Nachrichtenkategorie " unerwünscht" eine Nachricht dem Benutzer des ersten Empfängers E1 bereitgestellt werden soll. Ist dies der Fall, kann der Benutzer des zweiten
- 25 Empfängers E2 solche Nachrichten der Empfangseinrichtung ERW zuordnen (Schritt [12]).

- Vergleichbar dazu ist es dem Benutzer des zweiten Empfängers E2 möglich, auch auf unbekannte Nachrichten der
- 30 Empfangseinrichtung UNB zuzugreifen, unbekannte Nachrichten zu löschen oder gegebenenfalls der Empfangseinrichtung ERW bereitzustellen (Schritte [14] und [16]).

- Die Erfindung ist nicht nur in Email-Systemen und Email-
- 35 Diensten, insbesondere in sog. FreeMail-Diensten, einsetzbar, sondern in jedem Kommunikationssystem, in dem Nachrichten empfangen werden, so z.B. auch in Mobilkommunikationssystemen und -diensten. In diesem Zusammenhang kann z.B. der erste Empfänger der
- 40 Mobilkommunikations-Account eines Kindes sein und der

zweite Empfänger der Mobilkommunikations-Account eines  
Elternteils (Vater oder Mutter des Kindes). Bei eingehenden  
SMS- oder MMS-Nachrichten, die an das Kind bzw. an seinen  
Account gerichtet sind, wird vom zweiten Empfänger aus  
5 geprüft, ob die Nachrichten erwünscht sind oder nicht. Das  
geschieht z.B. anhand der Mobilfunk-Nummer des Sendenden  
(Calling Party Number). Der Elternteil kann den Zugriff auf  
nicht erwünschte SMS und/oder MMS sperren, so dass das Kind  
davor geschützt ist.

**PATENTANSPRÜCHE**

- 5 1. Verfahren zur Überwachung von an einen ersten Empfänger  
(E1) adressierten Nachrichten, bei dem  
- der erste Empfänger (E1) so eingerichtet wird, dass  
er eine Empfangseinrichtung "unerwünscht" (UNE)  
aufweist,  
10 - der erste Empfänger (E1) so eingerichtet wird, dass  
Zugriffe eines Benutzers des ersten Empfängers (E1) auf  
die Empfangseinrichtung "unerwünscht" (UNE) verhindert  
werden,  
- eine Nachrichtenkategorie "unerwünscht" definiert  
15 wird, die Nachrichten angibt, für die verhindert werden  
soll, dass sie einem Benutzer des ersten Empfängers  
(E1) bereitgestellt werden,  
- überprüft wird, ob eine an den ersten Empfänger (E1)  
adressierte Nachricht (M) in die Nachrichtenkategorie  
20 "unerwünscht" fällt,  
- die Nachricht (M) der Empfangseinrichtung  
"unerwünscht" (UNE) zugeordnet wird, wenn die Nachricht  
(M) in die Nachrichtenkategorie "unerwünscht" fällt,  
und  
25 - der erste Empfänger (E1) so eingerichtet wird, dass  
auf die Empfangseinrichtung "unerwünscht" (UNE) nur  
durch einen zweiten Empfänger (E2) zugegriffen werden  
kann.
- 30 2. Verfahren nach Anspruch 1, bei dem  
- der erste Empfänger (E1) so eingerichtet wird, dass  
er eine Empfangseinrichtung "erwünscht" (ERW) aufweist,  
- der erste Empfänger (E1) so eingerichtet wird, dass  
35 Zugriffe eines Benutzers des ersten Empfängers (E1) auf  
die Empfangseinrichtung "erwünscht" (ERW) zugelassen  
werden,  
- eine Nachrichtenkategorie "erwünscht" definiert wird,  
die Nachrichten angibt, die einem Benutzer des ersten  
40 Empfängers (E1) bereitgestellt werden,



1AP20 Rec'd PCT/PTO 21 APR 2006

- überprüft wird, ob die an den ersten Empfänger (E1) adressierte Nachricht (M) in die Nachrichtenategorie "erwünscht" fällt, und
  - die Nachricht (M) der Empfangseinrichtung "erwünscht" (ERW) zugeordnet wird, wenn die Nachricht (M) in die Nachrichtenategorie "erwünscht" fällt.
3. Verfahren nach Anspruch 1 oder 2, bei dem
- der erste Empfänger (E1) so eingerichtet wird, dass er eine Empfangseinrichtung "unbekannt" (UNB) aufweist,
  - der erste Empfänger (E1) so eingerichtet wird, dass Zugriffe eines Benutzers des ersten Empfängers (E1) auf die Empfangseinrichtung "unbekannt" (UNB) verhindert werden,
  - eine Nachrichtenategorie "unbekannt" definiert wird, die Nachrichten angibt, die nicht in die Nachrichtenategorie "unerwünscht" und nicht in die Nachrichtenategorie "erwünscht" fallen.
  - überprüft wird, ob die an den ersten Empfänger (E1) adressierte Nachricht (M) in die Nachrichtenategorie "unbekannt" fällt, und
  - die Nachricht (M) der Empfangseinrichtung "unbekannt" (UNB) zugeordnet wird, wenn die Nachricht (M) in die Nachrichtenategorie "unbekannt" fällt.
4. Verfahren nach Anspruch 3, bei dem der erste Empfänger (E1) so eingerichtet wird, dass auf die Empfangseinrichtung "unbekannt" (UNB) nur durch den zweiten Empfänger (E2) zugegriffen werden kann.
5. Verfahren nach einem der vorherigen Ansprüche, bei dem der erste Empfänger (E1) so eingerichtet wird, dass Änderungen der Nachrichtenategorie "unerwünscht" durch einen Benutzer des ersten Empfängers (E1) verhindert werden und die Definition der Nachrichtenategorie "unerwünscht" nur durch den zweiten Empfänger (E2) durchgeführt werden kann.
6. Verfahren nach einem der Ansprüche 3 bis 5, bei dem der erste Empfänger (E1) so eingerichtet wird, dass

- Änderungen der Nachrichtenkatgorie "unbekannt" durch einen Benutzer des ersten Empfängers (E1) verhindert werden und die Definition der Nachrichtenkatgorie "unbekannt" nur durch den zweiten Empfänger (E2) durchgeführt werden kann.
- 5
7. Verfahren nach einem der Ansprüche 4 bis 6, bei dem
- Nachrichten in der Empfangseinrichtung "unerwünscht" unter Verwendung des zweiten Empfängers (E2) kontrolliert werden, und
- 10
- kontrollierte Nachrichten unter Steuerung des zweiten Empfängers (E2) der Empfangseinrichtung "erwünscht" (ERW) zugeordnet werden.
8. Verfahren nach einem der Ansprüche 4 bis 7, bei dem
- Nachrichten in der Empfangseinrichtung "unbekannt" (UNB) unter Verwendung des zweiten Empfängers (E2) kontrolliert werden, und
- 15
- kontrollierte Nachrichten unter Steuerung des zweiten Empfängers (E2) der Empfangseinrichtung "erwünscht" (ERW) zugeordnet werden.
- 20
9. Verfahren nach einem der vorherigen Ansprüche, bei dem als erster Empfänger (E1) ein erster E-Mail-Account verwendet wird, dem als Empfangseinrichtung "unerwünscht" ein Ordner "Unerwünscht" (UNE) zugeordnet wird.
- 25
10. Verfahren nach einem der Ansprüche 2 bis 9, bei dem als erster Empfänger (E1) ein erster E-Mail-Account verwendet wird, dem als Empfangseinrichtung "erwünscht" ein Ordner "erwünscht" (ERW) zugeordnet wird.
- 30
11. Verfahren nach einem der Ansprüche 3 bis 10, bei dem als erster Empfänger (E1) ein erster E-Mail-Account verwendet wird, dem als Empfangseinrichtung "unbekannt" ein Ordner "unbekannt" (UNB) zugeordnet wird.
- 35

12. Verfahren nach einem der Ansprüche 4 bis 11, bei dem als zweiter Empfänger (E2) ein zweiter E-Mail-Account verwendet wird.
- 5 13. Verfahren nach einem der vorherigen Ansprüche, bei dem das Überprüfen der an den ersten Empfänger (E1) adressierten Nachricht vor einer Übertragung zu dem ersten Empfänger (E1) durchgeführt wird.
- 10 14. Verfahren nach einem der vorherigen Ansprüche, bei dem zum Überprüfen der an den ersten Empfänger (E1) adressierten Nachricht eine Wahrscheinlichkeit ermittelt wird, wonach die Nachricht in die Nachrichtenkategorie "unerwünscht" fällt.
- 15 15. Verfahren nach einem der Ansprüche 2 bis 14, bei dem zum Überprüfen der an den ersten Empfänger (E1) adressierten Nachricht eine Wahrscheinlichkeit ermittelt wird, wonach die Nachricht in die
- 20 Nachrichtenkategorie "erwünscht" fällt.
16. Verfahren nach einem der vorherigen Ansprüche, bei dem zum Überprüfen der Nachricht ein Spamfilter verwendet wird.
- 25 17. System zur Überwachung von an einen ersten Empfänger (E1) adressierten Nachrichten, mit
- einem ersten Empfänger (E1), der eine Empfangseinrichtung "unerwünscht" (UNE) aufweist und so
  - 30 eingerichtet ist, dass Zugriffe eines Benutzers des ersten Empfängers (E1) auf die Empfangseinrichtung "unerwünscht" (UNE) verhindert werden,
  - einem zweiten Empfänger (E2) zum Definieren einer Nachrichtenkategorie "unerwünscht", die Nachrichten
  - 35 angibt, für die verhindert werden soll, dass sie einem Benutzer des ersten Empfängers (E1) bereitgestellt werden, und
  - einer Einrichtung zur Überprüfung, ob eine an den ersten Empfänger (E1) adressierte Nachricht (M) in die
  - 40 Nachrichtenkategorie "unerwünscht" fällt, und um die

Nachricht (M) der Empfangseinrichtung "unerwünscht" (UNE) zuzuordnen, wenn die Nachricht (M) in die Nachrichten-kategorie "unerwünscht" fällt, wobei der erste Empfänger (E1) so eingerichtet ist, dass auf die Empfangseinrichtung "unerwünscht" (UNE) nur durch den zweiten Empfängers (E2) zugegriffen werden kann.

18. System nach Anspruch 17, bei dem
- 10 - der erste Empfänger (E1) eine Empfangseinrichtung "erwünscht" aufweist und so eingerichtet ist, dass Zugriffe eines Benutzers des ersten Empfängers (E1) auf die Empfangseinrichtung "erwünscht" (ERW) zugelassen werden,
  - 15 - der zweiten Empfänger (E2) zum Definieren einer Nachrichten-kategorie "erwünscht" eingerichtet ist, die Nachrichten angibt, die einem Benutzer des ersten Empfängers (E1) bereitgestellt werden sollen, und
  - 20 - die Überprüfungseinrichtung zur Überprüfung eingerichtet ist, ob die an den ersten Empfänger (E1) adressierte Nachricht (M) in die Nachrichten-kategorie "erwünscht" fällt, und eingerichtet ist, um die Nachricht (M) der Empfangseinrichtung "erwünscht" (ERW) zuzuordnen, wenn die Nachricht (M) in die
  - 25 Nachrichten-kategorie "erwünscht" fällt.

19. System nach Anspruch 17 oder 18, bei dem
- der erste Empfänger (E1) eine Empfangseinrichtung "unbekannt" (UNE) aufweist und so eingerichtet ist, dass Zugriffe eines Benutzers des ersten Empfängers (E1) auf die Empfangseinrichtung "unbekannt" (UNB) verhindert werden,
  - der zweiten Empfänger (E2) zum Definieren einer Nachrichten-kategorie "unbekannt" eingerichtet ist, die Nachrichten angibt, die nicht in die
  - 35 Nachrichten-kategorie "unerwünscht" und nicht in die Nachrichten-kategorie "erwünscht" fallen, und
  - die Überprüfungseinrichtung zur Überprüfung eingerichtet ist, ob die an den ersten Empfänger (E1) adressierte Nachricht (M) in die Nachrichten-kategorie
  - 40

"unbekannt" fällt, und eingerichtet ist, um die Nachricht (M) der Empfangseinrichtung "erwünscht" (ERW) zuzuordnen, wenn die Nachricht (M) in die Nachrichten-kategorie "erwünscht" fällt.

5

20. System nach Anspruch 19, bei dem der erste Empfänger (E1) so eingerichtet ist, dass auf die Empfangseinrichtung "unbekannt" (UNB) nur durch den zweiten Empfänger (E2) zugegriffen werden kann.

10

21. System nach einem der Ansprüche 17 bis 20, bei dem der zweite Empfänger (E2) ein zweiter E-Mail-Account ist.

15

22. System nach einem der Ansprüche 17 bis 21, bei dem die Überprüfungseinrichtung einen Filter umfasst, der die an den ersten Empfänger (E1) adressierte Nachricht (M) in Nachrichten-kategorie "unerwünscht" kategorisiert, wenn die Nachricht (M) in die Nachrichten-kategorie "unerwünscht" fällt.

20

23. System nach einem der Ansprüche 17 bis 22, bei dem die Überprüfungseinrichtung einen Filter umfasst, der die an den ersten Empfänger (E1) adressierte Nachricht (M) in Nachrichten-kategorie "erwünscht" kategorisiert, wenn die Nachricht (M) in die Nachrichten-kategorie "erwünscht" fällt.

25

24. System nach einem der Ansprüche 17 bis 23, bei dem die Überprüfungseinrichtung einen Filter umfasst, der die an den ersten Empfänger (E1) adressierte Nachricht (M) in Nachrichten-kategorie "unbekannt" kategorisiert, wenn die Nachricht (M) in die Nachrichten-kategorie "unbekannt" fällt.

30


35

25. System nach Anspruch 24, bei dem der Filter ein Spamfilter ist.

40

FreeMail-Header

Sie sind hier: WEB.DE > Dienste > FreeMail
Namevon Parent@web.de











**Hallo Christian Kunz**  
 Sie haben 66 ungelesene E-Mails  
 Unbekannt: 20 - Unerwünscht: 45  
 E-Mails: 150  
 WEB.Cent: 450 Aufladen undverwalten  
 Sie waren zuletzt am 12.08.03 um 11:54 angemeldet.

32 von 100 MB Speicher erweitern

Club-News: .....

**Neu: Design-Mails jetzt auch mit Musik**

 <p><b>E-Mail schreiben</b>          SMS, Fax, Grußkarte,          Mypage ändern</p>	 <p><b>Posteingang</b>          Neu:Kinderschutz          Spam-Schutz, Ordner, E-Mail Check</p>
 <p><b>Telefonieren</b>          Com.Win 1.8 mit          optimiertem Interface          und erweiterter          Kontaktsynchronisation</p>	 <p><b>Organizer</b>          Adressbuch, Gruppen,          Geburtstagsliste, Kalender,          Weckruf</p>
 <p><b>Friends &amp; Family</b>          Fotos, Videos, Musik mit          Freunden teilen...</p>	 <p><b>Extras</b>          E-Mail-Zentrale, Sicherheit,          Einstellungen, Filter,          Benachrichtigungen</p>

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice 

(c) WEB.DE 2003 -Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 1

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz verwalten

Kinder-Schutz verwalten

Aktivierte Kinderschutz-Konten

Hilfe

xyz@web.de

unerwünscht (12/10)

unbekannt (10/8)

deaktivieren

Webcents aufladen

testuser12@web.de

unerwünscht (12/10)

unbekannt (10/8)

deaktivieren

Webcents aufladen

Neuen Kinderschutz einrichten

Hilfe

Benutzername:  @web.de 

einrichten

Noch nicht aktivierte Kinderschutz-Konten

Hilfe

Adresse	Aktivator Key	
<input type="checkbox"/> abc@web.de	huxci0eze8rr	<a href="#">Löschen</a>
<input type="checkbox"/> testuser2@web.de	dhui9372323	<a href="#">Löschen</a>
<input type="checkbox"/> nochseintestuser@web.de	hu2i3087122	<a href="#">Löschen</a>
<input type="checkbox"/> nummer4@web.de	jhu2i3023478	<a href="#">Löschen</a>

☐ Alle Auswählen

löschen

Aktivierungsmail erneut senden

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status

Handbuch Kundenservice

(c) WEB.DE 2003 -Jobs bei WEB.DE

Machen Sie Ihre Homepage bekannt!

Fig. 2

FreeMail-Header	
Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz einrichten	
<b>Kinder-Schutz einrichten</b>	
<p>Sie möchten das Postfach &lt;Name&gt; in ein Kinderschutz-Postfach umwandeln. Der Inhaber dieses Postfaches erhält in Kürze eine Benachrichtigung per E-Mail. Folgende Schritte müssen noch ausgeführt werden, um die Aktivierung des Kinderschutz-Postfaches zu vollziehen:</p>	
<b>Schritt1:</b>	<a href="#">Hilfe</a>
<p>Durch Klick auf den Link, der sich in der Benachrichtigungsmail befindet, gelangt der Inhaber des umzuwandelnden Postfaches auf die Aktivierungsseite.</p>	
<b>Schritt2:</b>	<a href="#">Hilfe</a>
<p>Dort muss der Aktivator Key eingegeben werden, den nur Sie erhalten:</p> <p style="text-align: center;"><b>Aktivator Key: 72sdhbd</b></p> <p>Der Aktivator Key wird Ihnen außerdem auf der "Kinderschutz verwalten"-Seite im Bereich "noch nicht aktivierte Kinderschutz-Postfächer" angezeigt.</p>	
<b>Schritt3:</b>	<a href="#">Hilfe</a>
<p>Nach Eingabe des Aktivator Keys ist der Vorgang abgeschlossen und das neue Kinderschutz-Postfach ist eingerichtet. Dieses ist dann Ihrem Postfach zugeordnet.</p>	
<div style="border: 1px solid black; display: inline-block; padding: 5px 15px;">weiter</div>	
<div style="display: flex; justify-content: space-between;"><div>WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status</div><div>Handbuch  Kundenservice </div></div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"><div>(c) WEB.DE 2003 -Jobs bei WEB.DE</div><div>Machen Sie Ihre Homepage bekannt!</div></div>	

Fig. 3



FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinderschutz einrichten

Kinderschutz einrichten

Lieber FreeMail-Nutzer,

leider kann der Kinderschutz für das Postfach <Name> nicht eingerichtet werden, weil der Inhaber älter als 17 Jahre ist.

Falls Ihr Kind bei der Registrierung des Postfaches ein falsches Geburtsdatum angegeben hat, so muss diese zunächst korrigiert werden, bevor der Kinderschutz eingerichtet werden kann.

Das Geburtsdatum kann im Postfach des Kindes unter "Extras/Sicherheit/Nutzerdaten" verändert werden.

[zurück](#)

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice

(c) WEB.DE 2003 -Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 4

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz verwalten > Ordner NamevomKind@web.de

Unbekannt - Nachricht 1-10 von 10 Nachrichten
Montag, 11. Aug 2003

Posteingang
**Unbekannt (10/10)**
Unerwünscht (2/1)
Zum Patent angemeldet

So nutzen Sie den FreeMail Kinderschutz [Zurück zu meiner Startseite](#)

mein Kind davor schützen

meinem Kind zeigen

entfernen

Von	Betreff	Kinderschutz?	
<input type="checkbox"/> <Ichbindersexspammer@spam.hi>	Mal wieder was erleben?...	Mein Kind davor schützen            Meinem Kind zeigen	
<input type="checkbox"/> <titten@spam.hi>	Ruf an!...	Mein Kind davor schützen            Meinem Kind zeigen	
<input type="checkbox"/> <gabir@erootk.com>	Ich will Dich...	Mein Kind davor schützen            Meinem Kind zeigen	
<input type="checkbox"/> <LustundLiebe@sexworld.de.vu>	Blasmusik und mehr...	Mein Kind davor schützen            Meinem Kind zeigen	

☐ Alle Auswählen

Nachricht 1-4 von 10
 

◀ zurück
weiter ▶

mein Kind davor schützen

meinem Kind zeigen

entfernen

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice

(c) WEB.DE 2003 -Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 5

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz verwalten > E-Mail lesen
NamevomKind@web.de

E-Mail lesen
Montag, 11. Aug 2003

Nachricht 1 von 20 im Ordner Unbekannt
[Zurück zu meinem Postfach](#)

Entfernen

Mein Kind davor schützen

Meinem Kind zeigen

<b>Betreff:</b>	noch ein Test	<a href="#">erweiterten Header anzeigen</a> - <a href="#">kompakt anzeigen</a>
<b>Von:</b>	mir	
<b>An:</b>	mich	
<b>Datum:</b>	11.08.03 19:00:42	

Blablabla,  
das ist eine Mail.  
Bla.

Entfernen

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice

(c) WEB.DE 2003 - Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 6

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz deaktivieren

Kinder-Schutz deaktivieren

Lieber FreeMail-Nutzer,

Sie beabsichtigen, das Kinderschutz-Kont&Name> zu deaktivieren. Damit wird das betreffende Postfach wieder zu einem normalen FreeMail-Postfach mit vollem Funktionsumfang.

Zudem sind wieder sämtliche E-Mail-Ordner sichtbar, wodurch sämtliche Nachrichten wieder zugänglich sind, die an dieses Postfach gesendet werden.

Möchten Sie fortfahren?

abbrechen

weiter

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice


(c) WEB.DE 2003 - Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 7

FreeMail-Header

---

Sie sind hier: [WEB.DE](#) > [Dienste](#) > [FreeMail](#) NamevomKind@web.de









**Hallo Christian Kunz**  
 Du hast 66 ungelesene E-Mails  
 E-Mails: 150  
 WEB.Cent: 450 verwalten - aufladen  
 Du warst zuletzt am 12.08.03 um 11:54 angemeldet.

32 von 100 MB Speicher  
 erweitern



So, für diesen Kasten müssen wir uns noch irgendwas einfallen lassen. Vielleicht Klingeltöne oder irgend etwas anderes. Sollte zur angepeilten Zielgruppe passen.

**Neu: Design-Mails Jetzt auch mit Musik**

 <p><b>E-Mail schreiben</b>          SMS, Fax, Grußkarte,          Mypage ändern</p>	 <p><b>Posteingang</b>          Ordner, E-Mail Check</p>
 <p><b>SMS</b>          Alle SMS-Dienste auf          einen Blick</p>	 <p><b>Organizer</b>          Adressbuch, Gruppen,          Geburtstagsliste, Kalender,          Weckruf</p>
 <p><b>Friends &amp; Family</b>          Fotos, Videos, Musik mit          Freunden teilen...</p>	 <p><b>Extras</b>          E-Mail-Zentrale, Sicherheit,          Einstellungen, Filter,          Benachrichtigungen</p>

Hier kommt dann noch der Verweis auf das Klingel- und Logo-Portal hin

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status
Handbuch 
Kundenservice 

(c) WEB.DE 2003 -Jobs bei WEB.DE
Machen Sie Ihre Homepage bekannt!

Fig. 8

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinder-Schutz aktivieren

Kinder-Schutz aktivieren

Lieber FreeMail-Nutzer,

auf dieser Seite können Sie Ihr FreeMail-Konto<Name> zum Kinderschutz-Konto umstellen. Das zugehörige Elternkonto, dem dieses Konto zugeordnet werden soll, lautet<Name> und gehört<Vor- und Nachname>. Um die Umstellung zu vollziehen, geben Sie bitte unten den Aktivator Key ein, den der Inhaber des Elternkontos erhalten hat.

**Kinderschutz-Konto aktivieren** Hilfe

**Aktivator Key:**

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status Handbuch  Kundenservice

(c) WEB.DE 2003 -Jobs bei WEB.DE Machen Sie Ihre Homepage bekannt!

Fig. 9

FreeMail-Header

Sie sind hier: WEB.DE > FreeMail > Kinderschutz wird aktiviert

Kinderschutz wird aktiviert

Lieber FreeMail-Nutzer,

der Kinderschutz für Ihr Postfach wird aktiviert. Der Vorgang ist in etwa einer Stunde abgeschlossen. Danach können Sie wieder auf Ihr Postfach zugreifen.

[zur WEB.DE Startseite](#)

Promofläche

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status Handbuch  Kundenservice

(c) WEB.DE 2003 -Jobs bei WEB.DE Machen Sie Ihre Homepage bekannt!

Fig. 10

FreeMail-Header


Sie sind hier: WEB.DE > FreeMail > Kinderschutz deaktiviert

Kinderschutz deaktiviert

Lieber FreeMail-Nutzer,



der Kinderschutz für Ihr Postfach wurde deaktiviert, da Sie das 18. Lebensjahr vollendet haben. Sie verfügen jetzt über ein normales FreeMail-Postfach und können sämtliche Funktionen nutzen.

Außerdem haben Sie Zugriff auf die Ordner "Unbekannt" und "Unerwünscht".

 [zur Startseite](#)

---

WEB.DE - Suche - Dienste - FreeMail - Hilfe - Status

Handbuch  Kundenservice 

---

(c) WEB.DE 2003 -Jobs bei WEB.DE

Machen Sie Ihre Homepage bekannt!

Fig. 11

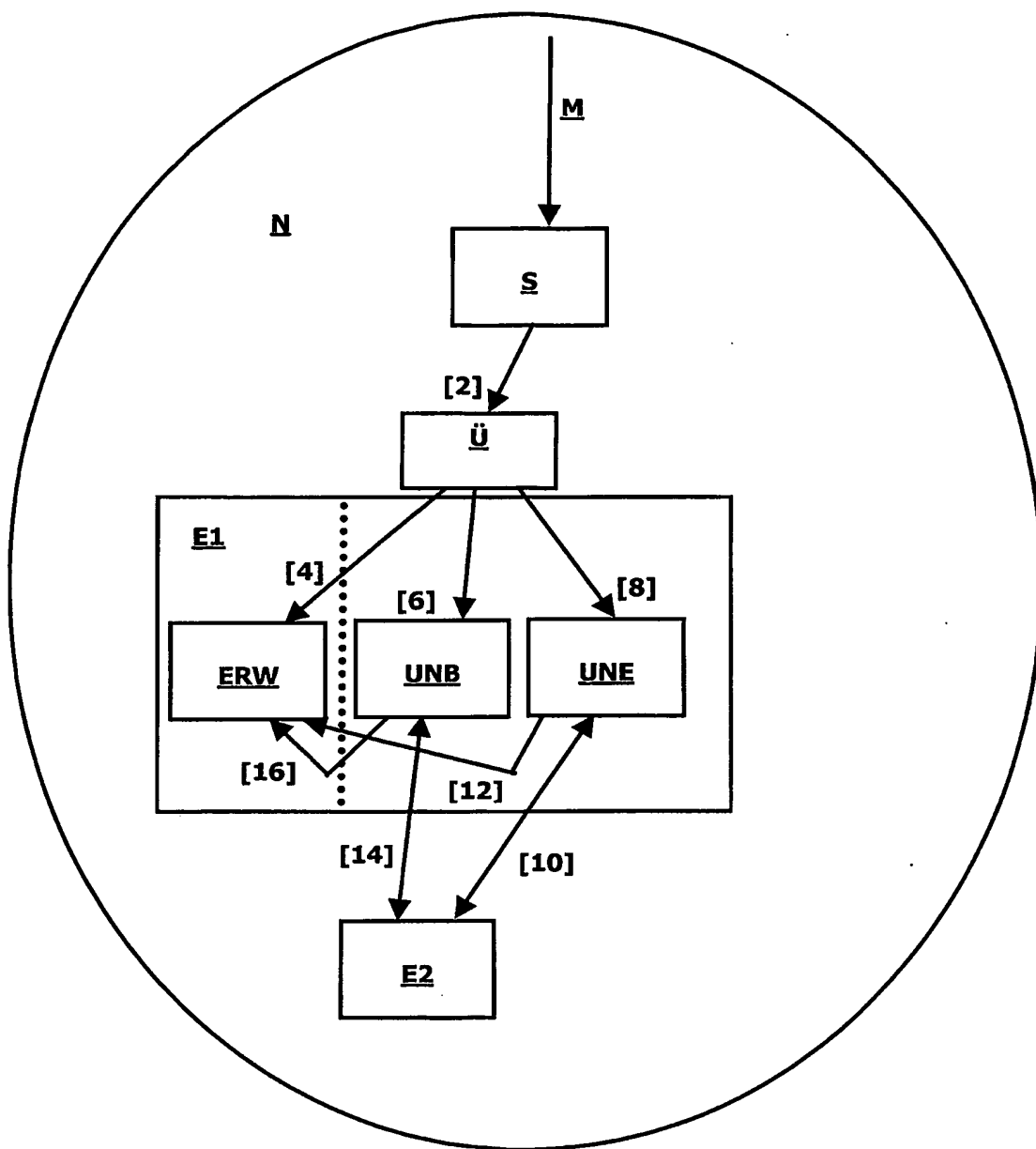


Fig. 12

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP2004/011934

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/199095 A1 (BANDINI JEAN-CHRISTOPHE ET AL) 26 December 2002 (2002-12-26) cited in the application	1-11, 13-25
Y	paragraphs '0021!', '0037!', '0038!'; figure 4	12
X	US 2002/107950 A1 (LU LARRY L) 8 August 2002 (2002-08-08)	1,2,13, 16-18, 21,24,25
Y	paragraphs '0003!', '0016!', '0019! - '0023!'; figure 2	12
X	US 6 393 464 B1 (DIETERMAN JUDE GERARD) 21 May 2002 (2002-05-21)	1,2,13, 16-18, 24,25
A	column 1, line 41 - line 49 column 3, line 35 - line 47 column 5, line 24 - line 46 figure 5	5-7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the International filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the International filing date but later than the priority date claimed

- \*T\* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*G\* document member of the same patent family

Date of the actual completion of the International search

10 March 2005

Date of mailing of the International search report

17/03/2005

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Frey, R

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/011934

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002199095 A1	26-12-2002	US 6609196 B1	19-08-2003
		US 2003196098 A1	16-10-2003
		US 2004193922 A1	30-09-2004
		US 2002169954 A1	14-11-2002
		US 2004054886 A1	18-03-2004
		AU 8759098 A	16-02-1999
		CA 2301147 A1	04-02-1999
		EP 1010283 A2	21-06-2000
		JP 2001518724 T	16-10-2001
		WO 9905814 A2	04-02-1999
US 2002107950 A1	08-08-2002	WO 02054211 A1	11-07-2002
US 6393464 B1	21-05-2002	AU 4997400 A	21-11-2000
		WO 0068815 A1	16-11-2000

BEST AVAILABLE COPY



# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/011934

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
IPK 7 H04L12/58

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2002/199095 A1 (BANDINI JEAN-CHRISTOPHE ET AL) 26. Dezember 2002 (2002-12-26) in der Anmeldung erwähnt	1-11, 13-25
Y	Absätze '0021!', '0037!', '0038!; Abbildung 4	12
X	US 2002/107950 A1 (LU LARRY L) 8. August 2002 (2002-08-08)	1,2,13, 16-18, 21,24,25
Y	Absätze '0003!', '0016!', '0019!' - '0023!; Abbildung 2	12
X	US 6 393 464 B1 (DIETERMAN JUDE GERARD) 21. Mai 2002 (2002-05-21)	1,2,13, 16-18, 24,25
A	Spalte 1, Zeile 41 - Zeile 49 Spalte 3, Zeile 35 - Zeile 47 Spalte 5, Zeile 24 - Zeile 46 Abbildung 5	5-7

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

\*A\* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

\*E\* älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist

\*L\* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

\*O\* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

\*P\* Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

\*T\* Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

\*X\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

\*Y\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

\*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

10. März 2005

Absenddatum des Internationalen Recherchenberichts

17/03/2005

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Frey, R

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/011934

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2002199095 A1	26-12-2002	US 6609196 B1	19-08-2003
		US 2003196098 A1	16-10-2003
		US 2004193922 A1	30-09-2004
		US 2002169954 A1	14-11-2002
		US 2004054886 A1	18-03-2004
		AU 8759098 A	16-02-1999
		CA 2301147 A1	04-02-1999
		EP 1010283 A2	21-06-2000
		JP 2001518724 T	16-10-2001
		WO 9905814 A2	04-02-1999
US 2002107950 A1	08-08-2002	WO 02054211 A1	11-07-2002
US 6393464 B1	21-05-2002	AU 4997400 A	21-11-2000
		WO 0068815 A1	16-11-2000